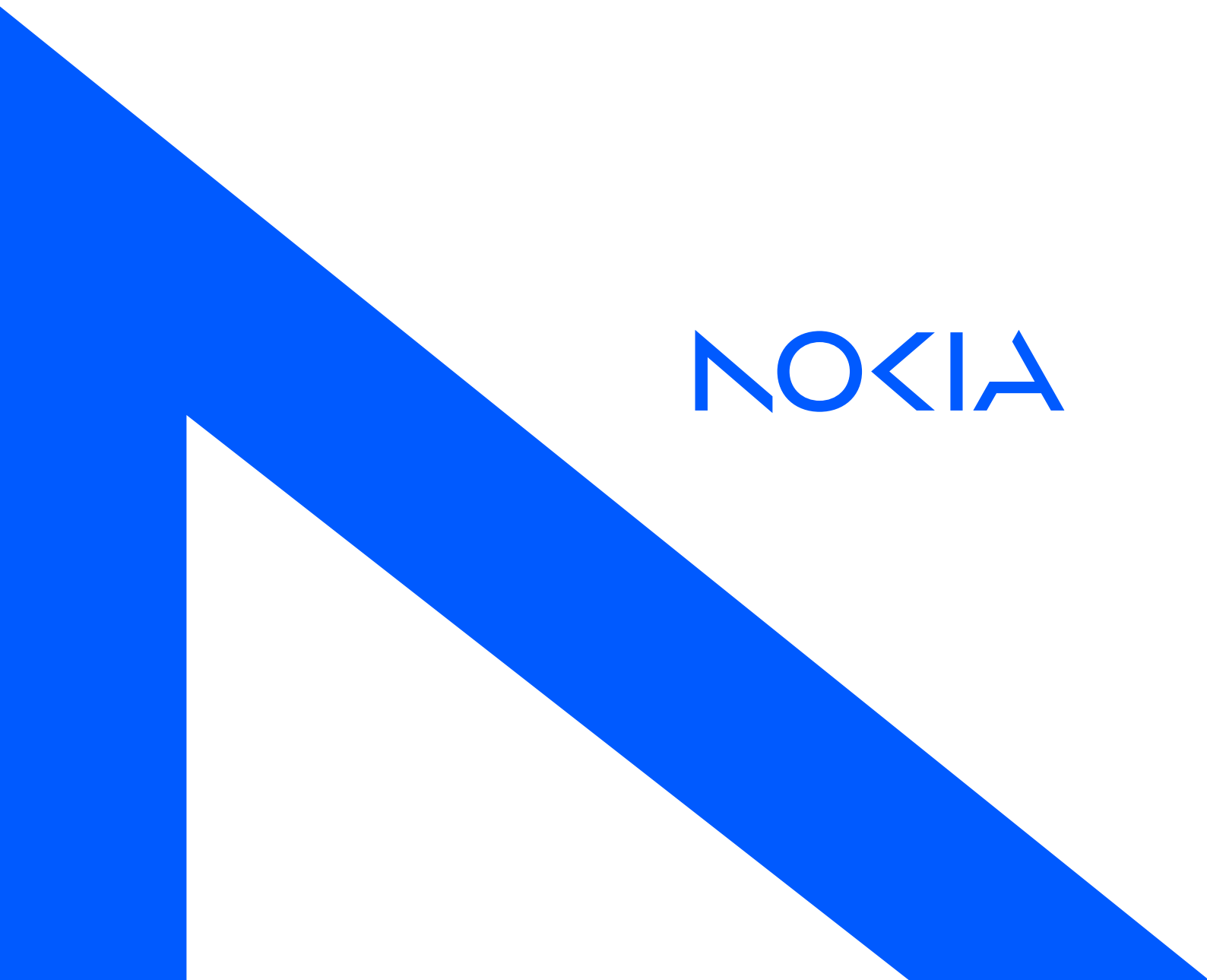
IPsec quantum-safe cryptography

Fortify your AI vision and digital transformation

Application note



Abstract

The exponential growth of data, rapid adoption of artificial intelligence (AI) and looming threat of quantum computing-enabled attacks are reshaping the way telecommunication, AI and cloud providers along with mission critical enterprises protect their networks.

Enter IPsec, the robust and proven protocol suite that's been quietly powering secure internet connections for decades, now evolving to meet the demands of today's hyperconnected landscape.

IPsec has long been a foundational security protocol and has now become a strategic enabler of secure and trusted digital transformation and AI investment. As organizations worldwide embrace cloud, remote work and Internet of Things (IoT), IPsec remains a cornerstone of encrypted communications.

The Nokia IPsec solution delivers a carrier-grade solution that secures IP traffic at layer 3 while seamlessly integrating with existing Nokia platforms (Nokia 7750 SR, 7705 SAR and Virtualized Service Router) or existing network infrastructures.

This battle-tested solution enables operators to deliver secure, high-availability network connectivity for remote-work VPNs, cloud interconnects, IoT, 5G backhaul, edge computing and cyber resilience. Its standards-based architecture, broad compatibility and proven security capabilities make it a critical enabler of trusted digital infrastructure.

Contents

Introduction

Networks and data have never been at greater risk. Most of the world's content and economies are becoming digitalized, which means that corporate, government and personal data traverses public and private networks in petabyte volumes. As the Quantum 2.0 era begins, the emergence of quantum computing presents a profound and urgent challenge to the cryptographic technologies that protect digital infrastructures. The threat is not hypothetical: Quantum computers will make widely used asymmetric cryptographic methods obsolete and expose organizations to systemic risk across their operations, supply chains and customer ecosystems.

The growing use of AI compounds this liability and changes the cyber threat landscape in potentially alarming ways. As enterprise and AI infrastructures become more distributed through multiple private data centers, distributed cloud services or a hybrid of the two, data spends more time in transit over public or private networks.

At the same time, the operators responsible for transporting these data flows are embracing open technologies, third-party transport options and globalization. These choices can make their networks more porous and vulnerable to attacks. Organizations are increasingly concerned about the confidentiality and integrity of data in flight or, more specifically, the growing vulnerability of data flows to interception and manipulation.

The challenge is clear: Organizations of all types need secure and trusted data connectivity to unlock the potential and value of investments in digitalization and AI.

Why IPsec is a guardian of the digital world

IPsec is a robust, battle-tested protocol suite that's been quietly powering secure internet connections for decades. It's now evolving to meet the demands of today's hyperconnected landscape.

IPsec is a suite of protocols defined by the Internet Engineering Task Force (IETF) for securing Internet Protocol (IP) communications at the network layer (layer 3 of the OSI model). It operates by authenticating and encrypting IP packets, ensuring confidentiality, integrity and authenticity without requiring modifications to higher-layer applications. Unlike application-layer security (e.g., Transport Layer Security, or TLS), IPsec provides end-to-end protection for any IP-based traffic.

Whether securing global VPNs for a remote workforce, shielding sensitive transactions across cloud platforms, protecting site-to-site network connections or locking down IoT ecosystems, IPsec delivers seamless, application-agnostic protection that ensures the confidentiality, integrity and authenticity of the data.

IPsec's market momentum is propelled by a confluence of global trends and urgent needs:

- **Escalating cyber threats**: With around 2,200 attacks occurring daily worldwide, businesses are prioritizing their defenses against ransomware, Advanced Persistent Threats and zero-days—driving IPsec adoption as a proven shield.
- **Digital transformation and cloud expansion**: The shift to hybrid work, multi-cloud environments and remote access demands secure connectivity. IPsec can support zero-trust models, which accelerate its growth in sectors such as IT and telecom.
- **Regulatory imperatives**: Stricter regulatory directives and data privacy laws (e.g., CCPA, GDPR, HIPAA, NIS2) mandate encrypted communications, creating compliance-driven demand.

- **IoT, 5G and edge computing**: As billions of devices connect via 5G networks, where device-to-cloud communication must be authenticated and encrypted. This is driving demand for IPsec into fast-growing markets such as smart cities and industrial IoT.
- **Technological advancements**: Innovations in quantum computing and AI cyber threats enhance IPsec's appeal because it can address future risks and meet the needs of forward-thinking telecommunication, AI and cloud providers and mission critical enterprises.

In essence, IPsec's market trajectory reflects its evolution from a foundational protocol to a cornerstone of secure and trusted network infrastructures.

IPsec adoption across networks

The use of IPsec continues to expand among telecommunication, AI and cloud providers and mission critical enterprises.

Table 1. IPsec applications for telecommunication providers and mission critical enterprises

Mission critical enterprise applications	Telecommunication provider applications
• Secure remote access for employees via IPsec VPNs • Branch office connectivity over public internet • Cloud interconnects between on-premises and cloud workloads • IoT device security in industrial and healthcare deployments	• Managed VPN services for enterprise customers • Secure backhaul for mobile and fixed networks • SD-WAN integration with IPsec tunnels for secure overlay • Carrier-grade encryption for critical infrastructure

IPsec is a cornerstone of secure networking, especially for telecommunication, AI and cloud providers and mission critical enterprises as they navigate the complexities of cloud transformation, remote work and cyber resilience. Its standards-based architecture, broad compatibility and proven security make it a critical enabler of secure and trusted digital infrastructure in the era of AI and quantum computing.

The Nokia IPsec solution

The Nokia IPsec solution (Figure 1) is available on the Nokia 7750 Service Router (SR), Nokia 7705 Service Aggregation (SAR) and Nokia Virtualized Service Router (VSR). These platforms can be implemented in centralized or distributed deployment models and come in several form factors to suit different business and application requirements. The IPsec solution functionality can be added to Nokia routers already deployed in a network or implemented with dedicated routers. To ensure high availability, the platforms can also be deployed in redundant configurations.

Figure 1. The Nokia IPsec platforms

7750 SR

Specialized cards are required in the 7750 SR platforms to support the IPsec solution functionality. Several Integrated Service Adapter (ISA) cards and external Extended Services Appliances (ESAs) are available to provide processing-intensive gateway services concurrently with other edge services, with no trade-offs between performance and advanced service delivery. The ISA cards and ESAs provide high-touch packet operations for advanced service capabilities, including IPsec and firewall.

Operators can extend the IPsec solution's flexible architecture by adding more ISA cards as half- or full-slot boards in a 7750 SR platform as IPsec traffic volumes increase. Alternatively, ESA modules connect to 100 GbE ports on 7750 SR routers, which saves slots on the routers. Up to 16 ISAs or ESAs can be added per 7750 SR router.

7705 SAR

Nokia offers IPsec solution capabilities on the 7705 SAR series of routers. For remote locations, IPsec clients enabled on the 7705 can use Ethernet-based services or wireless wide area network (WAN) access with cellular or wireless local area network (WLAN) access to provide IPsec secured connectivity. For hub locations, operators can use the new 7705 SAR Gen 2 platforms to provide a high-performance IPsec Security Gateway function. The 7705 SAR offers VPN capabilities tied to dedicated IPsec tunnels as either IPsec client or IPsec Security Gateway over the internet, wireless services or backup carrier services to provide a highly resilient and secure network architecture. Nokia offers a wide variety of 7705 SAR platforms to optimize remote and hub IPsec applications.

Virtualized Service Router

For operators that want to move more quickly to cloud technologies, Nokia delivers the IPsec solution functionality as a virtualized network function (VNF) on the industry-leading Nokia Virtualized Service Router (VSR). The IPsec solution application on the VSR leverages the cloud scalability of the x86 server architecture to accelerate cryptographic computation. Operators can scale up by adding more CPU and memory resources and scale out by adding more virtual machine resources. The application uses Intel QuickAssist Technology (QAT)to offload IPsec cryptography computation and significantly increase IPsec throughput.

Quantum-safe IPsec

We are entering the Quantum 2.0 era, where new quantum technologies will have significant and far-reaching benefits, but also consequences. As the development of quantum computers accelerates, we are approaching a critical inflection point where what the industry calls a cryptographically relevant quantum computer (CRQC) could soon be available. The CRQC will make most current asymmetric mathematics-based cryptography schemes obsolete, including Rivest–Shamir–Adleman (RSA), Diffie-Hellman (DH) key exchange and elliptic-curve cryptography (ECC). This threatens the integrity of digital infrastructures and economies because the industry has largely defaulted to these asymmetric cryptography solutions over the past several decades.

The availability date of a CRQC—often referred to as Q-Day—is the subject of market debate. But threat actors are already preparing for Q-Day. Many are collecting encrypted data from targeted organizations today and storing it so they can decrypt it when they eventually gain access to a CRQC. The industry refers to this ongoing activity as harvest now, decrypt later (HNDL). Network operators need to take steps now to secure their networks and mitigate this risk.

CRQCs impact IPsec in two areas but with different threat models:

1. Key exchange is used to derive the all the keys used by IPsec, including packet encryption keys. A threat actor can save encrypted IPsec traffic for future decryption with a CRQC in an HNDL attack.
2. Public key infrastructure (PKI) authentication is used to authenticate IPsec peers. A threat actor with a CRQC could impersonate an IPsec peer by forging certificates to compromise live IPsec communications.

There is ongoing work in standardization organizations to extend IPsec for new mathematics-based post-quantum cryptography (PQC) algorithms. NIST has announced new PQC algorithms, and other organizations are also engaged in the development of PQC algorithms. Even with the announcement of these PQC algorithms, the work to absorb them into standards and operational cryptography frameworks will likely take several years. The time to achieve operational maturity should not be underestimated.

To provide a secure and trusted quantum-safe IPsec cryptography solution, Nokia is implementing a multidimensional approach that features:

- Post-quantum pre-shared keys (PPKs)
  - Key exchange: The implementation of RFC8784 enables the provisioning of additional post-quantum pre-shared keys (PPKs) with quantum-safe entropy. These keys are incorporated into the IKEv2 key derivation process and are considered quantum-safe against a CRQC.
  - Authentication: If feasible, pre-shared key (PSK) authentication could be used to mitigate any risk concerns.
- Quantum-safe cryptography (QSC) mathematical algorithms
  - Key exchange: The NIST post-quantum cryptography (PQC) identified CRYSTALS-KYBER (ML-KEM) algorithm can be implemented in a hybrid mode of operation that merges the strengths of the new PQC and legacy (such as Elliptic Curve Diffie-Hellman) mathematical algorithms to deliver quantum-safe protection against a CRQC.
  - Public key infrastructure (PKI) authentication: PKI authentication relies heavily on digital signatures. For example, NIST has identified two complementary signature schemes: a lattice-based option (Module-Lattice Digital Signature Algorithm) for efficiency and a hash-based option (Stateless Hash-Based Digital Signature Algorithm) for long-term security conservatism. Both support the three security levels, which allows PKI operators to match classical equivalents.
  - PKI authentication will take longer and presents a more multifaceted challenge that involves the wider ecosystem, including certificate authorities, APIs and software libraries. Hybrid approaches are being considered to merge the strengths of the new PQC signatures with legacy digital signature operations. Integration into standards is ongoing through activities in forums, such as the IETF.

Nokia is committed to providing a quantum-safe IPsec solution. It will migrate to new PQC solutions aligned to the adoption and integration of the appropriate PQC algorithms and also adopt other appropriate technologies.

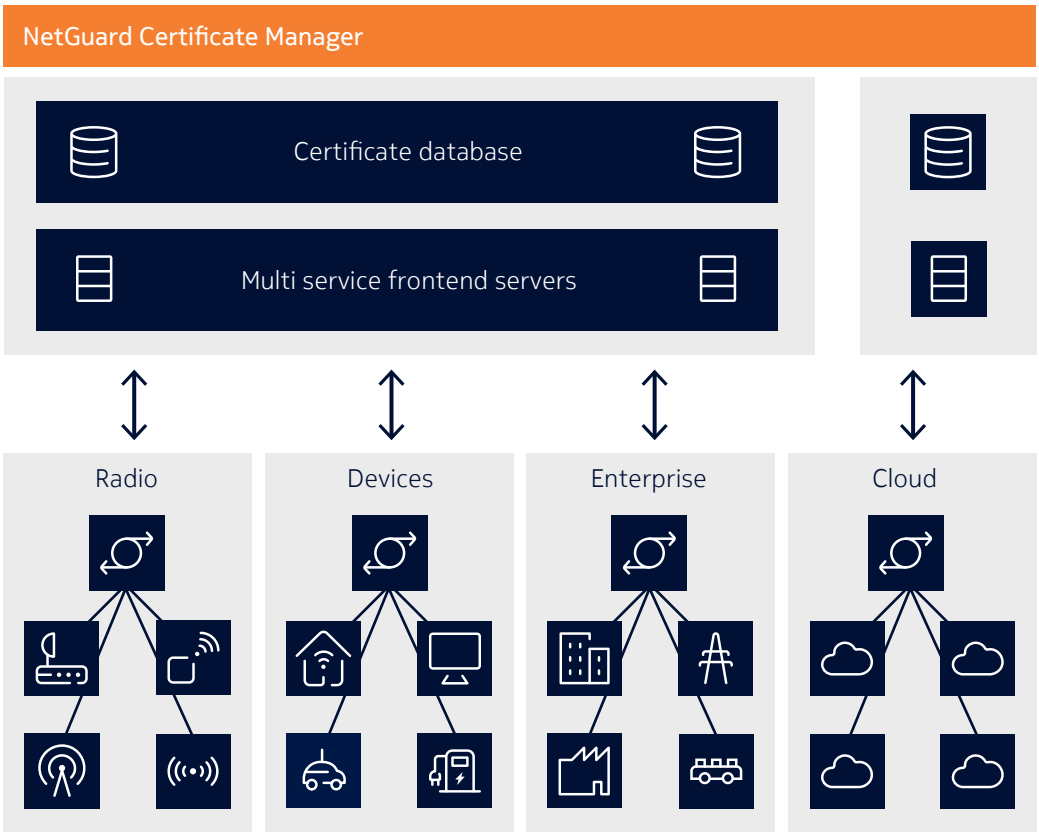
Certificate management

A trusted Certificate Authority (CA) provides the certificate used to authenticate a client's identity. The IPsec solution interoperates with industry-standard certificate managers, including the Nokia NetGuard Certificate Manager (NCM), which automates certificate enrolment and manages the full PKI certificate lifecycle. NCM is vendor-agnostic by design because it implements the industry standards for certificate enrolment and PKI operations.

When combined with the NCM, the IPsec solution provides the benefits of a complete PKI infrastructure. NCM supports the deployment of a full PKI hierarchy, including the root CA, intermediate or sub-CAs, and the issuance and lifecycle management of end-entity certificates, ensuring that every gateway and network element receives a verified and trusted digital identity.

NCM also offers deployment flexibility for different operational environments. It is used today by telecommunication providers, and mission critical enterprises, all of which require the highest levels of security and reliability. In large telecommunication provider networks, NCM supports a fully distributed and redundant architecture with high availability, Hardware Security Module (HSM) integration and offline root CA deployments. In smaller enterprise environments, it can be deployed on bare metal servers, virtual appliances, clouds or standard Kubernetes clusters while maintaining the same functional capabilities (Figure 2).

Figure 2. Nokia NetGuard Certificate Manager

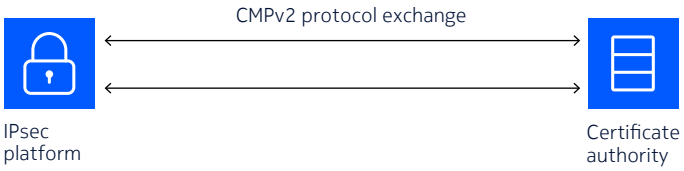


CMPv2 and EST

Certificate Management Protocol (CMPv2) and Enrollment over Secure Transport (EST) are two standard protocols that enable secure online communication between the IPsec platforms, acting as the end entity, and the CA.

These protocols allow the gateway to enroll for new certificates and renew existing ones, ensuring that certificate provisioning and updates are performed in a simple, automated and secure manner (Figure 3).

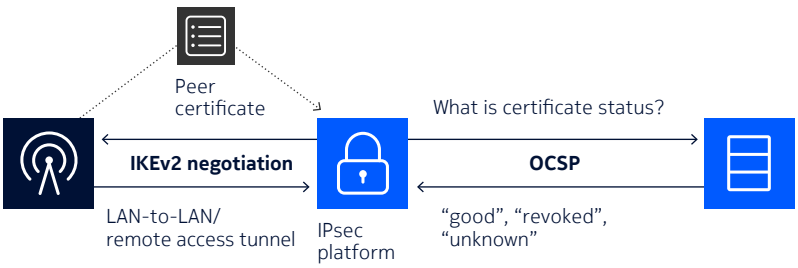
Figure 3. Support for CMPv2



OCSP

The IPsec platforms support the Online Certificate Status Protocol (OCSP), which enables real-time verification of a certificate's revocation status. By using OCSP, the gateway no longer depends on periodic certificate revocation list (CRL) updates and avoids the risk of operating with outdated revocation information (Figure 4).

Figure 4. Support for OCSP



Automatic certificate and CRL updates

Every certificate has a limited lifetime, and the CRL contains the revocation information issued by the CA. It is therefore essential to keep the certificate and the CRL up to date. The IPsec platforms support the following automatic update mechanisms:

- Certificate: The system automatically renews the certificate using the CMPv2 or EST protocol before the certificate expires.
- CRL: The system automatically downloads and updates the CRL from an HTTP server, either at regular intervals or before CRL expiration. These options make CRL management much easier for the network operator.

The Nokia advantage

Capacity and throughput

The Nokia IPsec solution has the industry's highest capacity and throughput. With the 7750 SR, there is support for up to 500,000 tunnels, with each ISA card or ESA-VM supporting up to 32,000 IPsec tunnels. The VSR can support 64,000 tunnels, and the 7705 SAR supports up to 4,000 tunnels. IPsec tunnel groups can be configured as required, with tunnel groups being load balanced across the available hardware resources.

Throughput can often be the more important parameter in network design. Each 7750 SR ISA2 card has a throughput of 40 Gb/s. The 7750 SR can take 16 ISA2 cards for a maximum throughput of 640 Gb/s per system. Each 7750 SR ESA-400G has 200 Gb/s IPsec throughput with up to 16 ESAs per system, for a maximum of 3.2 Tb/s throughput.

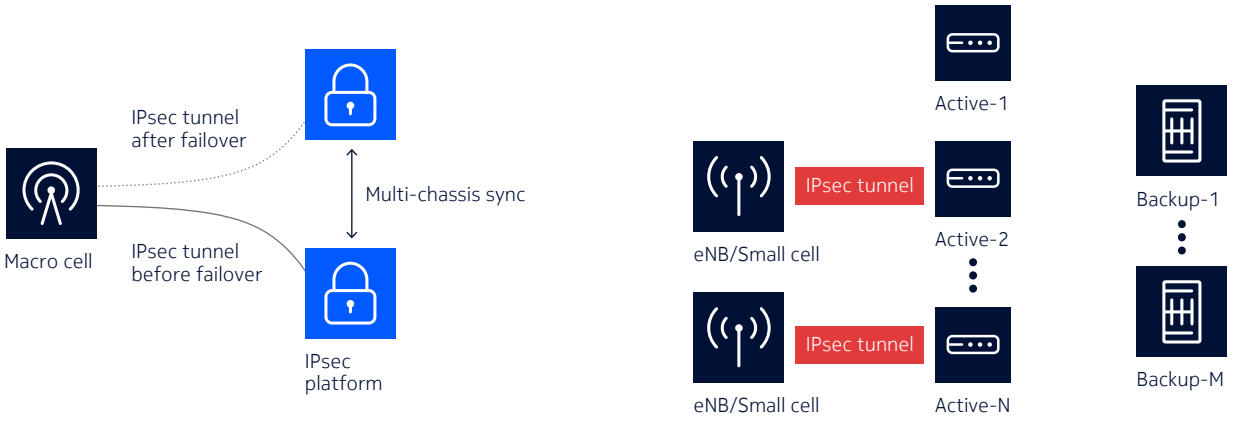
The Nokia VSR appliance option can support more than 100 Gb/s throughput, while the 7705 SAR supports up to 10 Gb/s throughput.

Carrier-grade high availability

High availability is often one of most important requirements for a network that supports digital transformation and AI applications. The IPsec solution meets stringent carrier-grade requirements for high availability with capabilities such as:

- N:M multi-chassis stateful IPsec redundancy (multi-chassis IPsec (MC-IPsec)), as shown in Figure 5.
- Carrier-grade non-stop routing and non-stop services.
- Load balancing at the port, card, service and tunnel levels.
- Fast convergence across technologies, including Bidirectional Forwarding Detection (BFD), Multiprotocol Label Switching (MPLS), Virtual Router Redundancy Protocol (VRRP), interior gateway protocols (IGPs) and Border Gateway Protocol (BGP).
- Fully redundant hardware components: control module, switch fabric, power and fan.
- High availability across control modules.

Figure 5. N:M multi-chassis redundancy



In multi-chassis stateful failover, all tunnel states are synchronized between multiple chassis or systems. Failover is fully transparent to the IPsec peer connected to the IPsec gateway. There is no need to renegotiate the tunnel and affect a service.

The immediate benefit for operators is that they can deploy radio sites based on a single IPsec tunnel (per service or for all services) instead of cumbersome, less scalable active/standby IPsec tunnels. They can do this while providing hitless service resiliency in case of a potential network or IPsec platform failure.

Because redundancy objectives and network characteristics can vary between different operators and different network builds, the IPsec solution offers multi-chassis stateful failover in an optimally flexible N:M mode. When N is reduced to 1, a single active chassis is assigned to one or more backup systems. This allows for sequential failover. For instance, a local system can fail over to a local system, which, in turn, fails to a remote system and so on. While this approach provides full redundancy irrespective of how much traffic flows through a protected system, it also requires the largest capital investment.

At the other end of the spectrum, reducing M to 1 allows any number of active systems to share a single designated backup. While this approach requires the smallest capital investment, the backup chassis can quickly become a congestion point if multiple failovers force it to address more traffic or tunnels than its rated capacity.

Operators often choose to sit somewhere in the middle, assigning multiple active systems to multiple backup systems so they can achieve the optimal balance point between cost and redundancy based on their unique network characteristics and redundancy objectives.

Full IPv6 support

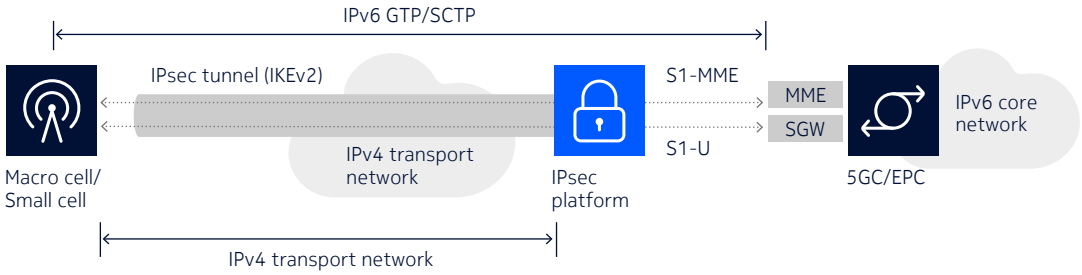
Operators are contending with rapidly growing ranks of user equipment (UE) and other access devices, along with growing adoption of IPv6 in these devices because of the depletion of IPv4 addresses. As a result, many networks need to evolve to IPv6 to support this adoption. While more operators are deploying IPv6, some parts of their networks may not yet support IPv6.

The Nokia IPsec solution addresses diverse network scenarios through comprehensive IPv6 support, including:

- IPv6 over IPv6
- IPv4 over IPv6
- IPv6 over IPv4
- IPv4 over IPv4.

This support gives network operators maximum flexibility for planning and rolling out IPv6 in their networks. For example, Figure 6 shows how the solution can support IPv6 over IPv4.

Figure 6. Support for IPv6 over IPv4 tunnels



Firewall

The IPsec solution is complemented by the firewall capability included in the Nokia Service Router Operating System (SR OS). This capability is designed to perform stateful, in-line packet inspection to stop unsolicited traffic from breaching the many secure zones required by today's open, distributed network architectures.

Nokia SR OS-based integrated firewalls sit in-line with traffic and track all sessions flowing into or out of the zone they protect. Flows solicited by legitimate users or applications pass through with rate limiting where required. Traffic not on a firewall's list of solicited flows is blocked. In addition, pinholes can be selectively enabled for trusted unsolicited traffic.

The stateful firewall supports a wide range of protocols, including Transmission Control Protocol (TCP) and GPRS Tunneling Protocol (GTP). It discards packets that violate protocol rules and neutralizes complex attacks that target the control, user and management planes of network functions and applications.

With high throughput and system modularity and scalability, Nokia SR OS firewalls are well-suited for deployment with the IPsec solution.

Integration with Nokia IP portfolio

Implementing the IPsec solution on the 7750 SR, 7705 SAR or VSR platforms offers many advantages. Nokia designed security into the SR OS software from the start and has proven its best-of-breed design credentials in telecommunication, AI and cloud providers and mission critical enterprises networks for 15-plus years.

The 7750 SR, 7705 SAR and VSR platforms enable the IPsec solution to use the full range of layer 2 and layer 3 services to seamlessly interoperate with IP/MPLS-based networks. Standard IP routing and MPLS protocols are used for interoperability, and the same operational and management models are used wherever a 7750 SR, 7705 SAR or VSR-based network is deployed.

With this flexibility, the IPsec Security Gateway and client functionality can be delivered in many different converged deployment scenarios to meet business and network application requirements. Many telecommunication providers and mission critical enterprises around the world have chosen to deploy the Nokia IPsec solution in diverse networking environments because of its ability to interwork with networking equipment from all major vendors.

Conclusion

The Nokia IPsec solution stands as a cornerstone for resilient, high-performance networking in an era defined by AI-driven workloads, massive data volumes and emerging quantum threats. By combining unmatched capacity, carrier-grade resilience, wide-ranging capabilities and a comprehensive quantum-safe strategy, this solution empowers telecommunication, AI and cloud providers and mission critical enterprises to protect critical traffic without sacrificing scalability or flexibility.

Integration with certificate automation, seamless IPv6 transition and built in stateful firewalling further reduce operational complexity, accelerate service rollout and ensure compliance with current and future security regulations. Whether deployed on dedicated hardware or as a VNF with the Nokia VSR, the solution delivers the same robust security posture across any deployment model—centralized, distributed or cloud-native.

By choosing the Nokia IPsec solution, telecommunication, AI and cloud providers along with mission critical enterprises get a future-ready security platform that mitigates current cyber risk and positions the network to withstand the quantumchallenges on the horizon, safeguarding digital transformation and AI investments for years to come.

Abbreviations

5GC	5G Core
AI	artificial intelligence
API	application programming interface
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BSC	Base Station Controller
BTSMED	base transceiver station mediator
CA	certificate authority
CCPA	California Consumer Privacy Act
CMPv2	Certificate Management Protocol
CPU	central processing unit
CRL	certificate revocation list
CRQC	cryptographically relevant quantum computer
DH	Diffie–Hellman
DU	distributed unit
ECC	elliptic-curve cryptography
eNB	Evolved Node B
EPC	Evolved Packet Core
ESP	Extended Services Appliance
EST	Enrolment over Secure Transport
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
HIPAA	Health Insurance Portability and Accountability Act
HNDL	harvest now, decrypt later
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security

ISA	Integrated Service Adapter
LAN	local area network
LTE	Long Term Evolution
MC-IPsec	multi-chassis IPsec
MME	Mobility Management Entity
MPLS	Multiprotocol Label Switching
NIS2	Network Information and Security Directive 2
NIST	National Institute of Standards and Technology
NSP	Network Services Platform
OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
OSS	operations support system
PKI	public key infrastructure
PPK	post-quantum pre-shared key
PQC	post-quantum cryptography
PSK	pre-shared key
QAT	QuickAssist Technology
QSC	quantum-safe cryptography
RAP	Radio Access Point
RNC	Radio Network Controller
RSA	Rivest–Shamir–Adleman
SAR	Service Aggregation Router
SCTP	Stream Control Transmission Protocol
SD-WAN	Software-Defined Wide Area Network
SeGW	security gateway
SGW	serving gateway
SR	Service Router
SRAN	Single RAN
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UE	user equipment
VNF	virtualized network function
VPN	virtual private network

VRRP	Virtual Router Redundancy Protocol
VSR	Virtualized Service Router
WAN	wide area network
WLAN	wireless LAN
WCDMA	Wideband Code Division Multiple Access

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (November) CID174280